ABSTRACT

The aim of this invention is to propose a control method for the conformity of a network key (NK). This method is applied during the transfer of data coming from a conditional access source to a domestic network. It handles on the verification of the network key (NK) authenticity using relevant control data provided by the verification center in general in form of a list $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$.

A verification of the presence or absence of a cryptogram $(TK)_{NK}$ is carried out according to the list $\{(TK)_{NK1}, (TK)_{NK2}, (TK)_{NK3} \ldots\}$. The cryptogram $(TK)_{NK}$ is constituted from a test key (TK), provided by the verification center, encrypted by a network key (NK) of a security module (CT) of a device (TV1, TV2, PC) connected to the network.

Figure 2